Groupe de travail Réseau
Request for Comments : 4513
RFC rendues obsolètes : 2251, 2829, 2830
Catégorie : Normes
Juin 2006

Auteur : R. Harrison, Novell, Inc.

Traduction : Claude Brière de L'Isle

Protocole léger d'accès à un répertoire (LDAP) :Méthodes d'authentification et mécanismes de sécurité

Statut de ce mémo

Le présent document spécifie un protocole de normalisation Internet pour la communauté de l'Internet, qui appelle à la discussion et à des suggestions pour son amélioration. Prière de se reporter à l'édition en cours des "Normes de protocole officielles de l'Internet" (STD 1) sur l'état de la normalisation et le statut de ce protocole. La distribution du présent mémo n'est soumise à aucune restriction.

Notice de Copyright

Résumé

Le présent document décrit les méthodes d'authentification et les mécanismes de sécurité du protocole léger d'accès à un répertoire (LDAP, *Lightweight Directory Access Protocol*). Il précise l'établissement de la sécurité de couche Transport (TLS) au moyen de l'opération StartTLS.
Le présent document précise la méthode d'authentification Bind simple y compris les mécanismes anonymes, non authentifié, et de nom/mot de passe et la méthode d'authentification Bind de couche simple d'authentification et de sécurité (SASL, *Simple Authentication and Security Layer*) qui inclus le mécanisme EXTERNAL.

Le présent document discute des divers états d'authentification et d'autorisation à travers lesquels peut passer une session vers un serveur LDAP et les actions qui déclanchent ces changements d'état.

Le présent document, conjointement avec les autres documents de la spécification technique LDAP (voir la Section 1 de la feuille de route de la spécification), rend obsolètes les RFC 2251, RFC 2829, et RFC 2830.

Table des matières

1 Introduction

Le protocole léger d'accès à des répertoires (LDAP, *Lightweight Directory Access Protocol*) [RFC4510] est un protocole puissant pour accéder à des répertoires. Il offre des moyens de recherche, de restitution et de manipulation de contenus de répertoires et des moyens d'accès un riche ensemble de fonctions de sécurité.

Il est vital que ces fonctions de sécurité soient interopérables entre tous les client et serveurs LDAP sur l'Internet ; il faut donc qu'il y ait un sous-ensemble minimum de fonctions de sécurité communes à toutes les mises en œuvre qui revendiquent la conformité à LDAP.

Les menaces de base qui pèsent sur un service de répertoires LDAP incluent (sans s'y limiter) :

(1) L'accès non autorisé à des données de répertoire via des opérations de restitution de données.

(2) L'accès non autorisé à des données de répertoire via par la surveillance de l'accès d'autres personnes.

(3) L'accès non autorisé à des informations réutilisables d'authentification de client en surveillant l'accès d'autres personnes.

(4) La modification non autorisée de données de répertoires.

(5) La modification non autorisée d'informations de configuration.

(6) Le déni de service : utilisation de ressources (habituellement en excès) de façon à refuser intentionnellement le service aux autres personnes.

(7) Usurpation : Tromper un utilisateur ou client en lui faisant croire que les informations viennent du répertoire alors qu'en fait, elle n'en proviennent pas, en modifiant des données en transit ou en dirigeant la connexion de transport du client sur une mauvaise adresse. Tromper un utilisateur ou client en envoyant des informations sensibles à une entité hostile qui semble être le serveur de répertoire mais ne l'est pas. Tromper un serveur de répertoire en lui faisant croire que des informations sont venues d'un client particulier alors qu'en fait elles viennent d'une entité hostile.

(8) Détournement : Un attaquant prend le contrôle d'une session de protocole établie.

Les menaces (1), (4), (5), (6), (7), et (8) sont des attaques actives. Les menaces (2) et (3) sont des attaques passives.

Les menaces (1), (4), (5), et (6) sont dues à des clients hostiles. Les menaces (2), (3), (7), et (8) sont dues à des agents hostiles sur le chemin entre le client et le serveur ou des agents hostiles se faisant passer pour un serveur, par exemple, une usurpation IP.

LDAP offre les mécanismes de sécurité suivants :

(1) Authentification au moyen de l'opération Bind. L'opération Bind fournit une méthode simple qui prend en charge les mécanismes anonyme, non authentifié, et nom/mot de passe, et la méthode de couche simple d'authentification et de sécurité (SASL, *Simple Authentication and Security Layer*), qui accepte une grande variété de mécanismes d'authentification.

(2) Des mécanismes pour prendre en charge des capacités de contrôle d'accès spécifiques du fabriquant (LDAP n'offre pas de capacité de contrôle d'accès standard).

(3) Le service d'intégrité des données au moyen de couches de sécurité dans les mécanismes de sécurité de couche Transport (TLS) ou SASL.

(4) Le service de confidentialité des données au moyen des couches de sécurité dans les mécanismes TLS ou SASL.

(5) La limitation d'utilisation de ressource de serveur au moyen de limites administratives configurées sur le serveur.

(6) L'authentification du serveur au moyen des mécanismes du protocole TLS ou de SASL.

LDAP peut aussi être protégé par des moyens en-dehors du protocole LDAP, par exemple, avec la sécurité de couche IP [RFC4301].

L'expérience a montré que permettre simplement aux mises en œuvre de choisir au hasard les mécanismes de sécurité qui seront mis en œuvre n'est pas une stratégie conduisant à l'interopérabilité. En l'absence d'obligations, les clients continueront à se voir écrire qu'ils n'acceptent aucune des fonctions de sécurité prises en charge par le serveur, ou pire, qu'ils ne prennent en charge que des mécanismes qui procurent une sécurité inadaptée à la plupart des circonstances.

Il est souhaitable de permettre aux clients de s'authentifier en utilisant une diversité de mécanismes incluant des mécanismes où les identités sont représentées comme des noms distingués [X.501][RFC4512], en forme de chaîne [RFC4514], ou comme utilisé dans différents systèmes (par exemple, des noms d'utilisateur simple [RFC4013]). Parce que certains mécanismes d'authentification transmettent des accréditifs sous forme de texte en clair, et/ou ne fournissent pas de services de sécurité des données et/ou sont soumis à des attaques passives, il est nécessaire de s'assurer d'une interopérabilité sécurisée en identifiant un mécanisme de mise en œuvre obligatoire pour l'établissement de services de sécurité de la couche transport.

L'ensemble des mécanismes de sécurité fournis par LDAP et décrits dans le présent document est destiné à satisfaire les besoins de sécurité d'une large gamme de scénarios de développement tout en fournissant un haut niveau d'interopérabilité parmi des diverses mises en œuvre et développements de LDAP.

1.1 Relations avec les autres documents

Le présent document fait partie intégrante de la spécification technique LDAP [RFC4510].

Le présent document, conjointement avec les [RFC4510], [RFC4511], et [RFC4512], rend obsolètes la RFC 2251 dans sa totalité. Les paragraphes 4.2.1 (en partie) et 4.2.2 de la RFC 2251 sont rendus obsolètes par le présent document. L'appendice B.1 résume les changements substantiels apportés à la RFC 2251 par le présent document.

Le présent document rend obsolète la RFC 2829 dans sa totalité. L'appendice B.2 résume les changements de substance apportés à la RFC 2829 par le présent document.

Les sections 2 et 4 de la RFC 2830 sont rendues obsolètes par la [RFC4511]. Le reste de la RFC 2830 est rendu obsolète par le présent document. L'appendice B.3 résume les changements de substance apportés à la RFC 2830 par le présent document.

1.2 Conventions

Les mots clé "DOIT", "NE DOIT PAS", "DOIT", "DEVRAIT", "NE DEVRAIT PAS", "PEUT", et "FACULTATIF" dans le présent document sont à interpréter comme décrit dans la RFC 2119 [RFC2119].

Le terme "utilisateur" représente tout être humain ou entité d'application qui accède au répertoire en utilisant un client de répertoire. Un client de répertoire (ou client) est aussi appelé agent d'utilisateur de répertoire (DUA, *directory user agent*).

Le terme "connexion de transport" se réfère aux services de transport sous-jacents utilisés pour porter l'échange de protocole, ainsi que les associations établies par ces services.

Le terme "couche TLS" se réfère aux services TLS utilisés pour la fourniture des services de sécurité, ainsi qu'aux associations établies par ces services.

Le terme "couche SASL" se réfère aux services SASL utilisés pour la fourniture des services de sécurité, ainsi qu'aux associations établies par ces services.

Le terme "couche de message LDAP" se réfère aux services (PDU) de message LDAP utilisés pour fournir des services de répertoire, ainsi qu'aux associations établies par ces services.

Le terme "session LDAP" se réfère aux services combinés (connexion de transport, couche TLS, couche SASL, couche de message LDAP) et leurs associations.

En général, la terminologie sur la sécurité utilisée dans le présent document est cohérente avec les définitions fournies dans la [RFC2828]. En outre, plusieurs termes et concepts se rapportant à la sécurité, l'authentification, et l'autorisation sont présentés à l'Appendice A du présent document. Alors que la définition formelle de ces termes et concepts est en dehors du domaine d'application du présent document, leur compréhension est indispensable à celle du présent document. Les lecteurs qui ne sont pas familiarisés avec les concepts qui touchent à la sécurité sont invités à revoir l'Appendice A avant de lire le reste du présent document.

2 Exigences de mise en œuvre

Les mises en œuvre de serveur LDAP DOIVENT prendre en charge le mécanisme d'authentification anonyme de la méthode Bind simple (paragraphe 5.1.1).

Les mises en œuvre LDAP qui prennent en charge un mécanisme d'authentification autre que le mécanisme d'authentification anonyme de la méthode Bind simple DOIVENT prendre en charge le mécanisme d'authentification de nom/mot de passe de la méthode Bind simple (paragraphe 5.1.3) et DOITVEN être capables de protéger cette authentification de nom/mot de en utilisant TLS comme établi par l'opération StartTLS (Section 3).

Les mises en œuvre DEVRAIENT interdire l'utilisation du mécanisme d'authentification de nom/mot de passe par défaut lorsque des services de sécurité des données convenable ne sont pas en place, et qu'elles PEUVENT fournir d'autres services de sécurité des données convenables à utiliser avec ce mécanisme d'authentification.

Les mises en œuvre PEUVENT prendre en charge des mécanismes d'authentification supplémentaires. Certains de ces mécanismes sont exposés ci-dessous.

Les mises en œuvre de serveur LDAP DEVRAIENT prendre en charge l'assertion du client d'identité d'autorisation via le mécanisme SASL EXTERNAL (paragraphe 5.2.3).

Les mises en œuvre de serveur LDAP qui ne prennent en charge aucun mécanisme d'authentification autre que le mécanisme anonyme de la méthode Bind simple DEVRAIENT prendre en charge l'utilisation de TLS comme établie par l'opération StartTLS (Section 3). (Les autres serveurs DOIVENT prendre en charge TLS selon le second paragraphe de cette section.)

Les mises en œuvre qu prennent en charge TLS DOIVENT accepter la suite de chiffrement TLS_RSA_WITH_3DES_EDE_CBC_SHA et DEVRAIENT prendre en charge la suite de chiffrement TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA. La prise en charge de cette dernière suite de chiffrement est recommandée pour favoriser l'interopérabilité avec les mises en œuvre qui se conforment aux spécifications StartTLS LDAP plus anciennes.

3 Opération StartTLS

L'opération Start de sécurité de couche Transport (StartTLS) définie au paragraphe 4.14 de la [RFC4511] procure la capacité à établir TLS [RFC4346] dans une session LDAP.

L'objectif de l'utilisation du protocole TLS avec LDAP est de s'assurer de la confidentialité et de l'intégrité des données, et de fournir facultativement l'authentification. TLS fournit expressément ces capacités, quoique les services d'authentification de TLS ne soient disponibles pour LDAP qu'en combinaison avec la méthode d'authentification EXTERNAL de SASL (voir au paragraphe 5.2.3), et seulement si la mise en œuvre EXTERNAL de SASL choisit de faire usage des accréditifs de TLS.

3.1 Procédures d'établissement de TLS

Ce paragraphe décrit les procédures générales que doivent suivre les clients et les serveurs pour l'établissement de TLS. Ces procédures prennent en considération divers aspects de la couche TLS, y compris la découverte du niveau de sécurité résultant et l'assertion ode l'identité d'autorisation du client.

3.1.1 Séquençage de la demande StartTLS

Un client peut envoyer la demande étendue StartTLS à tout moment après l'établissement d'une session LDAP, sauf :

- lorsque TLS est déjà établis sur la session,
- lorsqu'une négociation SASLM multi-étape SASL est en cours sur la session, ou
- lorsqu'il y a des réponses en cours pour des demandes d'opération précédemment produites sur la session.

Comme décrit dans la [RFC4511], paragraphe 4.14.1, une violation (détectée) de l'une de ces exigences a pour résultat le retour du code de résultat operationsError.

Les mises en œuvre de client devraient s'assurer qu'elles suivent strictement ces exigences de séquencement d'opérations pour empêcher les problèmes d'interopérabilité. L'expérience du fonctionnement a montré que violer ces exigences cause des problèmes d'interopérabilité à cause des conditions de concurrence qui empêchent les serveurs de détecter certaines violations de ces exigences du fait de facteurs tels que la vitesse des matériels serveurs et des délais de latence du réseau.

Il n'y a pas d'exigence générale que le client ait ou n'ait pas déjà effectué une opération Bind (Section 5) avant d'envoyer l'opération de demande StartTLS ; cependant, lorsqu'un client a l'intention d'effectuer à la fois une opération Bind et une opération StartTLS, il DEVRAIT d'abord effectuer l'opération StartTLS de sorte que les messages de demande et réponse Bind soient protégés par les services de sécurité des données établis par l'opération StartTLS.

3.1.2 Certificat de client

Si un serveur LDAP exige ou demande qu'un client fournisse un certificat d'utilisateur durant la négociation TLS et que le client ne présente pas un certificat d'utilisateur convenable (par exemple, qui puisse être validé), le serveur peut utiliser une politique de sécurité locale pour déterminer s'il doit achever avec succès la négociation TLS.

Si un client qui a fourni un certificat convenable effectue ensuite une opération Bind en utilisant le mécanisme d'authentification SASL EXTERNAL (paragraphe 5.2.3), les informations contenues dans le certificat peuvent être utilisées par le serveur pour identifier et authentifier le client.

3.1.3 Vérification d'identité du serveur

Afin de prévenir des attaques par intrusion, le client DOIT vérifier l'identité du serveur (telle que présentée dans le message Certificate du serveur). Dans ce paragraphe, la compréhension par le client de l'identité du serveur (normalement, l'identité utilisée pour établir la connexion du transport) est appelée "l'identité de référence".

Le client détermine le type (par exemple, nom DNS ou adresse IP) de l'identité de référence et effectue une comparaison entre l'identité de référence et chaque valeur subjectAltName du type correspondant jusqu'à produire une correspondance. Une fois la correspondance produite, l'identité du serveur a été vérifiée, et la vérification de l'identité du serveur est terminée. Différents types de subjectAltName sont comparés de différentes façons. Les paragraphes 3.1.3.1 à 3.1.3.3 expliquent comment comparer les valeurs des divers types subjectAltName.

Le client peut transposer l'identité de référence en un type différent avant d'effectuer une comparaison. Les transpositions peuvent être effectuées pour tous les types de subjectAltName disponibles pour lesquels l'identité de référence peut être transposée ; cependant, l'identité de référence ne devrait être transposée que dans des types pour lesquels la transposition est sécurisée par nature (par exemple, extraire le nom DNS d'un URI pour le comparer avec un subjectAltName de type dNSName) ou pour lesquels la transposition est effectuée de façon sécurisée (par exemple, en utilisant DNSSEC, ou en utilisant des tableaux de recherche d'hôte à adresse /adresse à hôte configurées par l'utilisateur ou par l'administration).

L'identité du serveur peut aussi être vérifiée en comparant l'identité de référence à la valeur du nom commun (CN, *Common Name*) [RFC4519] dans la feuille du nom distingué relatif (RDN, *Relative Distinguished Name*) du champ subjectName du certificat du serveur. Cette comparaison est effectuée en utilisant les règles de comparaison des noms DNS au paragraphe 3.1.3.1 ci-dessous, avec l'exception qu'aucune correspondance de caractère générique n'est acceptée. Bien que l'utilisation de la valeur du nom commun soit une pratique courante, elle est déconseillée, et les autorités de certification sont encouragées à fournir à la place des valeurs de subjectAltName. Noter que la mise en œuvre TLS peut représenter des DN dans des certificats, conformément à X.500 ou d'autres conventions. Par exemple, certaines mises en œuvre de X.500 ordonnent des RDN dans un DN en utilisant une convention de gauche à droite (du plus fort poids au plus faible poids) au lieu de la convention LDAP de droite à gauche.

Si la vérification de l'identité du serveur échoue, les clients orientés utilisateur DEVRAIT notifier l'utilisateur (les clients peuvent dans ce cas donner à l'utilisateur l'opportunité de continuer la session LDAP) ou fermer la connexion transport et indiquer que l'identité du serveur est suspecte. Les clients automatisés DEVRAIENT clore la connexion transport et retourner ou inscrire alors une erreur indiquant que l'identité du serveur est suspecte, ou les deux.

Au delà de la vérification de l'identité du serveur décrite dans ce paragraphe, les clients devrait être prêts à vérifier plus loin pour s'assurer que le serveur est autorisé à fournir le service qui lui est demandé. Le client peut avoir besoin d'utiliser des informations de politique locale pour le déterminer.

3.1.3.1 Comparaison des noms DNS

Si l'identité de référence est un nom de domaine international, les mises en œuvre conformes DOIVENT la convertir en format de codage compatible ASCII (ACE, ASCII Compatible Encoding) comme spécifié à la Section 4 de la RFC 3490 [RFC3490] avant la comparaison avec les valeurs subjectAltName de type dNSName. Précisément, les mises en œuvre conformes DOIVENT effectuer l'opération de conversion spécifiée à la Section 4 de la RFC 3490 comme suit :

* à l'étape 1, le nom de domaine DOIT être considéré comme une "chaîne mémorisée" ;
* à l'étape 3, établir le fanion appelé "UseSTD3ASCIIRules" ;
* à l'étape 4, traiter chaque étiquette avec l'opération "ToASCII" ; et
* à l'étape 5, changer tous les séparateurs d'étiquette en U+002E (point).

Après avoir effectué la conversion "en ASCII", les étiquettes et noms DNS DOIVENT être comparés en égalité conformément aux règles spécifiée à la Section 3 de la RFC3490.

Le caractère générique '*' (ASCII 42) est permis dans les valeurs de subjectAltName de type dNSName, et seulement comme étiquette DNS la plus à gauche (de moindre poids) dans cette valeur. Ce caractère générique correspond à toute étiquette DNS la plus à gauche dans le nom de serveur. C'est-à-dire, le sujet *.example.com correspond au nom de serveur a.example.com et b.example.com, mais ne correspond pas à example.com ou a.b.example.com.

3.1.3.2 Comparaison des adresses IP

Lorsque l'identité de référence est une adresse IP, l'identité DOIT être convertie à la représentation de chaîne d'octet dans "l'ordre des octets du réseau" [RFC791][RFC2460]. Pour IP Version 4, comme spécifié dans la RFC 791, la chaîne d'octet contiendra exactement quatre octets. Pour IP Version 6, comme spécifié dans la RFC 2460, la chaîne d'octet contiendra exactement seize octets. Cette chaîne d'octets est alors comparée aux valeurs de subjectAltName de type iPAddress. Une correspondance survient si la chaîne d'octet d'identité de référence et les chaînes d'octet de valeur sont identiques.

3.1.3.3 Comparaison des autres types de subjectName

Les mises en œuvre de client PEUVENT prendre en charge la confrontation avec des valeurs de subjectAltName d'autres types, comme décrit dans d'autres documents.

3.1.4 Découverte du niveau de sécurité résultant

Après qu'une couche TLS a été établie dans une session LDAP, les deux parties vont chacune indépendamment décider ou non de continuer sur la base de la politique locale et du niveau de sécurité atteint. Si toutes les parties décident que le niveau de sécurité est inadéquat à la poursuite de l'opération, elles DEVRAIENT retirer la couche TLS immédiatement après la fin de la (re)négociation TLS (voir la [RFC4511], le paragraphe 4.14.3, et le paragraphe 3.2 ci-dessous). Les mises en œuvre peuvent réévaluer le niveau de sécurité à tout moment, et, le trouvant inadéquat, devraient retirer la couche TLS.

3.1.5 Rafraîchissement des informations de capacité du serveur

Après l'établissement d'une couche TLS dans une session LDAP, le client DEVRAIT éliminer ou rafraîchir toutes les informations sur le serveur qu'il a obtenues avant l'initialisation de la négociation TLS et qu'il n'a pas obtenues par des

mécanismes sécurisés. Cela protège contre les attaques par intrusion qui peuvent avoir altéré toutes les informations sur les capacités de serveur récupérées avant l'installation de la couche TLS.

Le serveur peut faire connaître différentes capacités après l'installation d'une couche TLS. En particulier, la valeur de 'supportedSASLMechanisms' peut être différente après l'installation d'une couche TLS (précisément, les mécanismes EXTERNAL et PLAIN [PLAIN] ne seront mentionnés qu'après l'installation d'une couche TLS).

3.2 Effet de TLS sur l'état d'autorisation

L'établissement, le changement, et/ou la clôture de TLS peuvent causer le passage de l'état d'autorisation à un nouvel état. Ce point est approfondi à la Section 4.

3.3 Suites de chiffrement TLS

Plusieurs questions devraient être prises en considération lors du choix de suites de chiffrement TLS appropriées pour une utilisation dans des circonstances données. Parmi ces questions figurent celles qui suivent :

- La capacité de la suite de chiffrement à fournir une protection adéquate de la confidentialité pour les mots de passe et autres données envoyées sur la connexion transport. Les mises en œuvre de client et de serveur devrait être averties que certaines suites de chiffrement TLS ne procurent aucune protection de la confidentialité, alors que d'autres suites de chiffrement qui fournissent une protection de la confidentialité peuvent être vulnérables et peuvent être forcées en utilisant des méthodes brutales, particulièrement à la lumière des vitesses de CPU toujours croissantes qui réduisent le temps nécessaire pour monter de telles attaques avec succès.
- Les mises en œuvre de client et de serveur devraient considérer avec une grande attention la valeur du mot de passe ou des données protégée par rapport au niveau de protection de la confidentialité fournie par la suite de chiffrement pour s'assurer que le niveau de protection offert par la suite de chiffrement est approprié.
- La vulnérabilité (ou son absence) de la suite de chiffrement aux attaques par intrusion. Les suites de chiffrement vulnérables aux attaques par intrusion NE DEVRAIENT PAS être utilisées pour protéger des mots de passe ou des données sensibles, à moins que la configuration du réseau ne soit telle que le danger d'une attaque par intrusion soit négligeable.
- Après l'achèvement d'une négociation TLS (initiale ou ultérieure), les deux protocoles homologues devraient vérifier indépendamment que les services de sécurité fournis par la suite de chiffrement négociée sont adéquats pour l'utilisation prévue de la session LDAP. Si ils ne le sont pas, la couche TLS devrait être close.

4 État d'autorisation

Chaque session LDAP a un état d'autorisation associé. Cet état se compose de nombreux facteurs tels que (s'il en est) si l'état d'authentification a été établis, comment il l'a été, et quels services de sécurité sont en place. Certains facteurs peuvent être déterminés et/ou affectés par des événements de protocole (par exemple, Bind, StartTLS, ou la fermeture de TLS), et certains facteurs peuvent être déterminés par des événements externes (par exemple, l'heure du jour ou la charge du serveur).

Alors qu'il est souvent convenable de voir un état d'autorisation dans des termes simplistes (comme on le fait souvent dans la présente spécification technique) comme "un état anonyme", on note que les systèmes d'autorisation dans les mises en œuvre de LDAP implique habituellement de nombreux facteurs qui interagissent de façon complexe.

Dans LDAP, l'autorisation est une affaire locale. Un des facteurs clés dans la prise de décisions d'autorisation est l'identité d'autorisation. L'opération Bind (définie au paragraphe 4.2 de la [RFC4511] et exposée plus en détails à la Section 5 ci-dessous) permet que des informations soient échangée entre le client et le serveur pour établir une identité d'autorisation pour la session LDAP. L'opération Bind peut aussi être utilisée pour déplacer la session LDAP dans un état d'autorisation anonyme (voir au paragraphe 5.1.1).

Lors de l'établissement initial de la session LDAP, la session a une identité d'autorisation anonyme. Entre autres choses, cela implique que le client n'a pas besoin d'envoyer une BindRequest dans le premier PDU de la couche de message LDAP. Le client peut envoyer toute demande d'opération avant d'effectuer une opération Bind, et le serveur DOIT la traiter comme si elle avait été effectuée après une opération Bind anonyme (paragraphe 5.1.1).

A réception d'une demande Bind, le serveur passe immédiatement la session à un état d'autorisation anonyme. Si la demande Bind est réussie, la session est passée à l'état d'authentification demandé avec son état d'autorisation associé. Autrement, la session reste dans un état anonyme.
On note que d'autres événements à la fois internes et externes à LDAP peuvent avoir pour résultat que les états d'authentification et d'autorisation sont passés à l'état anonyme. Par exemple, l'établissement, le changement, ou la clôture de services de sécurité de données peut résulter en un passage à un état anonyme, ou bien les information d'accréditation de l'utilisateur (par exemple, le certificat) peuvent être arrivées à expiration. Le premier cas est un exemple d'événement interne à LDAP, alors que le dernier est un exemple d'événement externe à LDAP.

5 Opération Bind

L'opération Bind ([RFC4511], paragraphe 4.2) permet l'échange des informations d'authentification entre le client et le serveur pour établir un nouvel état d'autorisation.

La demande Bind spécifié normalement l'identité d'authentification désirée. Certains mécanismes Bind permettent aussi au client de spécifier l'identité d'autorisation. Si l'identité d'autorisation n'est pas spécifiée, le serveur la déduit de l'identité d'authentification d'une façon qui est spécifique de la mise en œuvre.

Si l'identité d'autorisation est spécifiée, le serveur DOIT vérifier que l'identité d'authentification du client est autorisée à supposer (par exemple, mandatée pour) l'identité d'autorisation certifiée. Le serveur DOIT rejeter l'opération Bind avec un code de résultat invalidCredentials dans la réponse Bind si le client n'y est pas autorisé.

5.1 Méthode d'authentification simple

La méthode d'authentification simple de l'opération Bind donne trois mécanismes d'authentification :
- Un mécanisme d'authentification anonyme (paragraphe 5.1.1).
- Un mécanisme d'authentification non authentifié (paragraphe 5.1.2).
- Un mécanisme d'authentification nom/mot de passe utilisant des accréditifs consistant en un nom (sous la forme d'un nom distinctif LDAP [RFC4514]) et un mot de passe (paragraphe 5.1.3).

5.1.1 Mécanisme d'authentification anonyme de Bind simple

Un client LDAP peut utiliser le mécanisme d'authentification anonyme de la méthode Bind simple pour établir explicitement un état d'autorisation anonyme en envoyant une demande Bind avec une valeur de nom de longueur zéro et en spécifiant le choix d'authentification simple contenant une valeur de mot de passe de longueur zéro.

5.1.2 Mécanisme d'authentification non authentifiée de Bind simple

Un client LDAP peut utiliser le mécanisme d'authentification non authentifié de la méthode Bind simple pour établir un état d'autorisation anonyme en envoyant une demande Bind avec une valeur de nom (un nom distinctif en forme de chaîne LDAP [RFC4514] de longueur différente de zéro) et en spécifiant le choix d'authentification simple contenant une valeur de mot de passe de longueur zéro.

La valeur de nom distinctif fournie par le client est destinée à n'être utilisée que pour les besoins du suivi (par exemple, journal d'enregistrement). La valeur n'est pas à authentifier ou autrement valider (y compris la vérification que le DN se réfère à un objet de répertoire existant). La valeur n'est pas à utiliser (directement ou indirectement) pour des besoins d'autorisation.

Les opérations Bind non authentifiées peuvent poser des problèmes de sécurité significatifs (voir au paragraphe 6.3.1). En particulier, les utilisateurs qui ont l'intention d'effectuer l'authentification par nom/mot de passe peuvent fournir par inadvertance un mot de passe vide et causer ainsi la demande d'accès non authentifié par les mises en œuvre de client désavantagés. Les clients DEVRAIENT être configurés pour demander la sélection par l'utilisateur du mécanisme d'authentification non authentifiée par des moyens autres que l'entrée par l'utilisateur d'un mot de passe vide. Les clients DEVRAIENT interdire l'entrée d'un mot de passe vide à l'interface d'utilisateur d'authentification par nom/mot de passe. De plus, les serveurs DEVRAIENT par défaut faire échouer les demandes Bind non authentifiées avec un code de résultat de unwillingToPerform *(refus d'exécuter).*

5.1.3 Mécanisme d'authentification par nom/mot de passe de Bind simple

Un client LDAP peut utiliser le mécanisme d'authentification nom/mot de passe la méthode Bind simple pour établir un état d'autorisation authentifié en envoyant une demande Bind avec une valeur de nom (un nom distinctif en forme de chaîne LDAP [RFC4514] de longueur différente de zéro) et en spécifiant le choix d'authentification simple contenant une valeur de mot de passe de CHAINE D'OCTET de longueur différente de zéro.

Les serveurs qui transposent le nom distinctif (DN) envoyé dans la demande Bind à une entrée de répertoire avec un ensemble associé d'un ou plusieurs mots de passe utilisés avec ce mécanisme compareront le mot de passe présenté à cet ensemble de mots de passe. Le mot de passe présenté est considéré comme valide si il correspond à un des membres de cet ensemble.

Un code de résultat *(resultCode)* de invalidDNSyntax indique que le DN envoyé dans la valeur de nom est de syntaxe invalide. Un code de résultat de invalidCredentials indique que le DN est correct en syntaxe mais n'est pas valide pour les besoins de l'authentification, que le mot de passe n'est pas valide pour le DN, ou que le serveur considère par ailleurs que les accréditifs sont invalides. Un code de résultat de succès indique que les accréditifs sont valides et que le serveur est d'accord pour fournir le service à l'entité identifiée par ces accréditifs.

Le comportement du serveur est indéfini pour les demandes Bind qui spécifient le mécanisme d'authentification de nom/mot de passe avec une valeur de nom de longueur zéro et une valeur de mot de passe de longueur différente de zéro.

Le mécanisme d'authentification de nom/mot de passe de la méthode Bind simple ne convient pas pour l'authentification dans les environnements sans protection de la confidentialité.

5.2 Méthode d'authentification SASL

La méthode d'authentification SASL de l'opération Bind fournit des facilités pour utiliser tout mécanisme SASL y compris les mécanismes d'authentification et les autres services (par exemple, services de sécurité des données).

5.2.1 Profil de protocole SASL

LDAP permet l'authentification via tout mécanisme SASL [RFC4422]. Comme LDAP inclut des méthodes d'authentification anonyme et par nom/mot de passe (texte en clair), les mécanismes SASL ANONYMOUS [RFC4505] et PLAIN [PLAIN] ne sont normalement pas utilisés avec LDAP.

Chaque protocole qui utilise les services SASL doit fournir certaines informations de profilage de la façon dont elles sont exposées à travers le protocole ([RFC4422], Section 4). Ce paragraphe explique comment chacune de ces exigences de profilage est satisfaite par LDAP.

5.2.1.1 Nom de service SASL pour LDAP

Le nom de service SASL pour LDAP est "ldap", qui a été enregistré auprès de IANA comme nom de service SASL.

5.2.1.2 Initialisation d'authentification et échange de protocole SASL

L'authentification SASL est initialisée via un message BindRequest message ([RFC4511], paragraphe 4.2) avec les paramètres suivants :
- La version est 3.
- Le choix d'authentification *(AuthenticationChoice)* est sasl.
- L'élément de mécanisme de la séquence SaslCredentials contient la valeur du mécanisme SASL désiré.
- Le champ facultatif d'accréditifs de la séquence SaslCredentials PEUT être utilisé pour fournir une réponse de client initiale pour les mécanismes qui sont définis comme ayant le client qui envoie les données en premier (voir la [RFC4422], Sections 3 et 5).

En général, un échange de protocole d'authentification SASL consiste en une série de mises en cause du serveur et de réponses du client, dont le contenu est spécifique du mécanisme SASL qui le définit. Et donc, pour certains mécanismes d'authentification SASL, il peut être nécessaire que le client réponde à un ou plusieurs mise en cause du serveur en envoyant plusieurs fois des messages BindRequest. Une mise en cause est indiquée par l'envoi par le

serveur d'un message BindResponse avec le resultCode (code de résultat) réglé à saslBindInProgress. Cela indique que le serveur réclame que le client envoie un nouveau message BindRequest avec le même mécanisme SASL pour continuer le processus d'authentification.

A la couche de message LDAP, ces mises en cause et réponses sont des jetons binaires opaques de longueur arbitraire. Les serveurs LDAP utilisent le champ serverSaslCreds (une CHAINE D'OCTETS) dans un message BindResponse pour transmettre chaque mise en cause. Les clients LDAP utilisent le champ accréditifs (une CHAINE D'OCTETS) dans la séquence SaslCredentials d'un message BindRequest pour transmettre chaque réponse. Noter qu'à la différence de certains protocoles Internet utilisant SASL, LDAP n'est pas fondé sur le texte et ne transforme pas en Base64 ces valeurs de mise en cause et de réponse.

Les clients qui envoient un message BindRequest en retenant le choix sasl DEVRAIENT envoyer une valeur de longueur zéro dans le champ de nom. Les serveurs qui reçoivent un message BindRequest en retenant le choix sasl DOIVENT ignorer toute valeur figurant dans le champ de nom.

Un client peut interrompre une négociation Bind SASL en envoyant in message BindRequest avec une valeur différente dans le champ de mécanisme de SaslCredentials ou avec un AuthenticationChoice autre que sasl.

Si le client envoie une BindRequest avec le champ mécanisme vide sous la forme d'une chaîne vide, le serveur DOIT retourner une BindResponse avec un resultCode de authMethodNotSupported. Ceci permet au client d'interrompre une négociation si il souhaite essayer à nouveau avec le même mécanisme SASL.

Le serveur indique l'achèvement de l'échange de mise en cause/réponse SASL en répondant par une BindResponse avec la valeur de resultCode différente de saslBindInProgress.

Le champ serverSaslCreds dans la BindResponse peut être utilisé pour inclure une mise en cause facultative avec notification de réussite pour les mécanismes qui sont définis pour que le serveur envoie des données supplémentaires avec l'indication de bon achèvement.

5.2.1.3 Champs facultatifs

Comme exposé ci-dessus, LDAP fournit un champ facultatif pour le transport de la réponse initiale dans le message qui initialise l'échange SASL et un champ facultatif pour porter des données supplémentaires dans le message qui indique le résultat de l'échange d'authentification. Comme dans ces champs, le contenu spécifique du mécanisme peut être de longueur zéro, SASL exige des spécifications de protocoles qu'elles détaillent la façon dont un champ vide se distingue d'un champ absent.

Les données de réponse initiale de longueur zéro ne se distinguent pas des données de réponse initiale dans le message d'initialisation, un PDU BindRequest, par la présence de la CHAINE D'OCTETS SaslCredentials.credentials (de longueur zéro) dans ce PDU. Si le client n'a pas l'intention d'envoyer une réponse initiale avec la BindRequest initialisant l'échange SASL, il DOIT omettre la CAHINE D'OCTETS SaslCredentials.credentials (plutôt que d'inclure une CHAINE D'OCTET de longueur zéro).

Les données supplémentaires de longueur zéro ne se distinguent pas des données de réponse supplémentaires dans le message de résultat, un PDU BindResponse, par la présence de la CHAINE D'OCTETS serverSaslCreds (de longueur zéro) dans ce PDU. Si un serveur n'a pas l'intention d'envoyer des données supplémentaires dans le message BindResponse qui indique le résultat de l'échange, le serveur DOIT omettre la CHAINE D'OCTETS serverSaslCreds (plutôt que d'inclure une CHAINE D'OCTET de longueur zéro).

5.2.1.4 Octet où prennent effet les couches de sécurité négociées

Les couches SASL prennent effet à la suite de la transmission par le serveur et de la réception par le client de la BindResponse finale dans l'échange SASL avec un code de résultat de succès.

Une fois que la couche SASL fournissant les services d'intégrité des données ou de confidentialité prend effet, la couche reste en effet jusqu'à l'installation d'une nouvelle couche (c'est-à-dire, au premier octet suivant la BindResponse finale de l'opération Bind qui a causé la prise d'effet de la nouvelle couche). Et donc, un couche SASL établie n'est pas affectée par un Bind échoué ou non-SASL.

5.2.1.5 Détermination des mécanismes SASL pris en charge

Les clients peuvent déterminer les mécanismes SASL pris en charge par un serveur en lisant l'attribut 'supportedSASLMechanisms' dans la racine DSE (entrée spécifique de DSA, *DSA specific Entry*) ([RFC4512], paragraphe 5.1). Les valeurs de cet attribut, s'il en est, font la liste des mécanismes pris en charge par le serveur dans l'état LDAP de la session en cours. Les serveurs LDAP DEVRAIENT permettre à tous les clients – même ceux qui ont une autorisation anonyme -- de restituer l'attribut 'supportedSASLMechanisms' du DSE racine à la fois avant et après l'échange d'authentification SASL. L'objet de cette dernière est de permettre au client de détecter une possible attaque par dégradation (voir le paragraphe 6.4 ci-dessous et le paragraphe 6.1.2 de la [RFC4422]).

Parce que les mécanismes SASL fournissent des fonctions de sécurité critiques, les clients et serveurs devraient être configurables de façon à spécifier quels mécanismes sont acceptables et ne permettre que ceux qui sont à utiliser. Les clients et serveurs doivent tous deux confirmer que le niveau de sécurité négocié satisfait leurs exigences avant de poursuivre l'utilisation de la session.

5.2.1.6 Règles d'utilisation des couches SASL

A l'installation d'une couche SASL, le client DEVRAIT éliminer ou rafraîchir toutes les informations sur le serveur qu'il a obtenues avant l'initialisation de la négociation SASL et qu'il n'a pas obtenues par des mécanismes sécurisés.

Si une couche de sécurité de niveau inférieur (telle que TLS) est installée, toute couche SASL DOIT être placée sur le dessus de telles couches de sécurité indépendamment de l'ordre de leur négociation. A tous les autres égards, la couche SASL et les autres couches de sécurité agissent indépendamment, par exemple, si une couche TLS et une couche SASL sont toutes deux en effet, le retrait de la couche TLS n'affecte pas la continuation du service de la couche SASL.

5.2.1.7 Prise en charge des authentifications multiples

LDAP prend en charge des authentifications SASL multiples, comme défini à la Section 4 de la [RFC4422].

5.2.1.8 Identités d'autorisation SASL

Certains mécanismes SASL permettent aux clients de demander une identité d'autorisation désirée pour la session LDAP ([RFC4422], Section 3.4). La décision de permettre ou interdire à l'identité d'authentification en cours d'avoir accès à l'identité d'autorisation demandée est une affaire de politique locale. L'identité d'autorisation est une chaîne de caractères[Unicode] codés en UTF-8 [RFC3629] correspondant à la grammaire de forme Backus-Naur augmentée (ABNF, *Augmented Backus-Naur Form*) [RFC4234] suivante :

```
authzId = dnAuthzId / uAuthzId

; distinguished-name-based authz id
dnAuthzId =  "dn:" distinguishedName

; unspecified authorization id, UTF-8 encoded
uAuthzId = "u:" userid
userid = *UTF8 ; syntax unspecified
```

où la règle distinguishedName est définie à la Section 3 de la [RFC4514] et la règle UTF8 est définie au paragraphe 1.4 de la [RFC4512].

Le choix dnAuthzId est utilisé pour établir les identités d'autorisation sous la forme d'un nom distinctif à faire correspondre conformément à la règle de correspondance distinguishedNameMatch du paragraphe 4.2.15 de la [RFC4517]. Il n'est pas exigé que la valeur du distinguishedName établi soit une entrée dans le répertoire.

Le choix uAuthzId permet aux clients d'établir une identité d'autorisation qui ne soit pas sous forme d'un nom distinctif. Le format de userid n'est défini que comme une séquence de caractères [Unicode] codés en UTF-8 [RFC3629], et toute interprétation ultérieure est une question locale. Par exemple, le userid pourrait identifier un utilisateur d'un service de répertoire spécifique, qu'il soit un nom de connexion, ou une adresse de messagerie électronique. Un uAuthzId NE DEVRAIT PAS être supposé être mondialement unique. Pour comparer des valeurs de uAuthzId, chaque valeur de uAuthzId DOIT être préparée comme une chaîne "query" *(d'interrogation)* de la Section 7

de la [RFC3454] en utilisant l'algorithme SASLprep [RFC4013], et ensuite deux valeurs sont comparées octet par octet.

La grammaire ci-dessus est extensible. La production de authzId peut être étendue pour prendre en charge des formes d'identité supplémentaires. Chaque forme est distinguée par son préfixe unique (voir le paragraphe 3.12 de la [RFC4520] pour les exigences d'enregistrement).

5.2.2 Sémantique de SASL au sein de LDAP

Les développeurs doivent veiller à maintenir la sémantique des spécifications SASL lors du traitement de données qui ont une sémantique différente dans le protocole LDAP.

Par exemple, le mécanisme d'authentification SASL DIGEST-MD5 [DIGEST-MD5] utilise une identité d'authentification et un domaine qui sont syntaxiquement de simples chaînes et sémantiquement de simples valeurs de nom d'utilisateur [RFC4013] et de domaine. Ces valeurs ne sont pas des DN LDAP, et il n'y a pas d'exigence qu'elles soient représentées ou traitées comme telles.

5.2.3 Mécanisme d'authentification SASL EXTERNAL

Un client peut utiliser le mécanisme SASL EXTERNAL ([RFC4422], Appendice A) pour demander au serveur LDAP d'authentifier et d'établir une identité d'autorisation résultante en utilisant les accréditifs de sécurité échangés par une couche de sécurité inférieure (comme l'authentification TLS). Si le les accréditifs d'authentification du client n'ont pas été établis à une couche de sécurité inférieure, Le Bind SASL EXTERNAL DOIT échouer avec un code de résultat de inappropriateAuthentication. Bien que cette situation ait pour effet de laisser la session LDAP dans un état anonyme (Section 4), l'état de tout couche de sécurité installée n'est pas affecté.

Un client peut demander que son identité d'autorisation soit automatiquement déduite de ses accréditifs d'authentification échangés à une couche de sécurité inférieure, ou il peut explicitement fournir une identité d'autorisation désirée. Le premier est appelé une assertion implicite, et le second une assertion explicite.

5.2.3.1 Assertion implicite

Une assertion implicite d'identité d'autorisation est effectuée en invoquant une demande Bind de forme SASL utilisant le nom de mécanisme EXTERNAL qui n'inclue pas le champ accréditifs facultatif (qui se trouve dans la séquence SaslCredentials dans la demande BindRequest). Le serveur déduira l'identité d'autorisation du client de l'identité d'authentification fournie par une couche de sécurité (par exemple, un certificat de clé publique utilisé durant l'installation de la couche TLS) conformément à la politique locale. Les mécanismes sous-jacents de réalisation sont spécifiques de la mise en œuvre.

5.2.3.2 Assertion explicite

Une assertion explicite d'identité d'autorisation est effectuée en invoquant une demande Bind de forme SASL utilisant le nom de mécanisme EXTERNAL qui inclue le champ accréditifs (qui se trouve dans la séquence SaslCredentials dans la demande BindRequest). La valeur du champ accréditifs (une CHAINE D'OCTETS) est l'identité d'autorisation prétendue et DOIT être construite comme expliqué au paragraphe 5.2.1.8.

6 Considérations sur la sécurité

Les questions de sécurité sont discutées tout au long du présent document. La conclusion attendue est que la sécurité est une partie intégrante et nécessaire de LDAP. La présente section discute un certain nombre de considérations sur la sécurité en rapport avec LDAP.

6.1 Considérations générales sur la sécurité de LDAP

LDAP ne fournit par lui-même ni sécurité ni protection de l'accès ou de la mise à jour du répertoire par des moyens autres qu'au travers du protocole LDAP, par exemple, par l'inspection des fichiers de base de données du serveur par les administrateurs de la base de données.

Les données sensibles peuvent être portées dans presque tous les messages LDAP, et leur révélation peut être soumise à des lois sur la confidentialité ou autres réglementations dans de nombreux pays. Les développeurs devraient prendre des mesures appropriées pour protéger les données sensibles contre leur révélation à des entités non autorisées.

Une session sur laquelle le client n'a pas établi de services de protection de l'intégrité des données et de la confidentialité (par exemple, via StartTLS, IPsec, ou un mécanisme SASL convenable) est l'objet d'attaques par intrusion pour voir et modifier les informations en transit. Les développeurs de client et de serveur DEVRAIENT prendre des mesures pour protéger les données sensibles dans la session LDAP contre ces attaques en utilisant des services de protection des données comme exposé dans le présent document. Les clients et serveurs devraient fournir la capacité d'être configurés pour exiger ces protections. Un code de résultat de confidentialityRequired indique que le serveur exige l'établissement d'une protection (plus forte) de la confidentialité de données afin d'effectuer l'opération demandée.

Le contrôle d'accès devrait toujours être appliqué lors de la lecture d'informations sensibles ou de la mise à jour d'information d'un répertoire.

Divers facteurs de sécurité, incluant les informations d'authentification et d'autorisation et les services de sécurité des données, peuvent changer durant le cours d'une session LDAP, ou même durant l'accomplissement d'une opération particulière. Les mises en œuvre devraient être robustes dans le traitement de facteurs de sécurité changeants.

6.2 Considérations sur la sécurité de StartTLS

Toute la sécurité gagnée par l'utilisation de l'opération StartTLS est obtenue de l'utilisation de TLS lui-même. L'opération StartTLS, par elle-même n'apporte aucune sécurité supplémentaire.

Le niveau de sécurité procuré par l'utilisation de TLS dépend directement à la fois de la qualité de la mise en œuvre de TLS utilisée et du style d'utilisation de cette mise en œuvre. De plus, un attaquent par intrusion peut retirer l'opération étendue StartTLS de l'attribut 'supportedExtension' du DSE racine. Les deux parties DEVRAIENT certifier de façon indépendante et consentir au niveau de sécurité réalisé une fois que TLS est établi et avant de commencer à utiliser la session protégée par TLS. Par exemple, le niveau de sécurité de la couche TLS peut avoir été négocié en texte clair.

Les clients DOIVENT soit avertir l'utilisateur lorsque le niveau de sécurité réalisé ne procure pas un niveau acceptable de confidentialité des données et/ou de protection de l'intégrité des données, soit avoir une configuration les mettant à même de refuser de continuer dans un niveau de sécurité acceptable.

Comme indiqué au paragraphe 3.1.2, un serveur peut utiliser une politique de sécurité locale pour déterminer s'il peut terminer avec succès une négociation TLS. Les informations qui sont contenues dans le certificat d'utilisateur qui est produit ou vérifié par l'autorité de certification devraient être utilisées par l'administrateur de la politique lors de la configuration de la politique d'identification et d'autorisation.

Les développeurs de serveurs DEVRAIENT permettre aux administrateurs de serveurs de décider quelle confidentialité et intégrité des données est exigée et quand elle l'est, ainsi que de décider si l'authentification du client est exigée durant la prise de contact TLS.

Les développeurs devraient être avertis des considérations de sécurité de TLS et les comprendre, telles qu'elles sont présentées dans la spécification TLS [RFC4346].

6.3 Considérations sur la sécurité de l'opération Bind

Ce paragraphe expose plusieurs considérations sur la sécurité pertinentes pour l'authentification LDAP via l'opération Bind.

6.3.1 Considérations sur la sécurité des mécanismes non authentifiés

L'expérience montre que les clients peuvent mésuser (et le font fréquemment) du mécanisme d'authentification non authentifié de la méthode Bind simple (voir au paragraphe 5.1.2). Par exemple, un programme client peut prendre une décision d'accorder l'accès à des informations qui ne sont pas celles d'un répertoire sur la base d'une opération Bind bien terminée. Les mises en œuvre de serveur LDAP peuvent retourner une réponse de succès à une demande Bind non authentifiée. Cela peut malencontreusement laisser au client l'impression que le serveur a réussi à authentifier l'identité

représentée par le nom distinctif alors qu'en réalité, c'est un état d'autorisation anonyme qui a été établi. Les clients qui utilisent les résultats d'un simple opération Bind pour prendre des décisions d'autorisation devraient détecter de façon active les demandes Bind non authentifiées (en vérifiant que le mot de passe fourni n'est pas vide) et réagir en conséquence.

6.3.2 Considérations sur la sécurité du mécanisme nom/mot de passe

Le mécanisme d'authentification nom/mot de passe de la méthode Bind simple dévoile le mot de passe au serveur, ce qui est un risque intrinsèque pour la sécurité. Il y a d'autres mécanismes, tels que SASL DIGEST-MD5 [DIGEST-MD5], qui ne révèlent pas le mot de passe au serveur.

6.3.3 Considérations sur la sécurité en rapport avec le mot de passe

LDAP permet des attributs de mot de passe multi valeurs. Dans les systèmes où les entrées sont supposées avoir un seul et unique mot de passe, les contrôles administratifs devraient être prévus pour mettre en application ce comportement.

L'utilisation de mots de passe en texte clair et autres accréditifs d'authentification non protégés est fortement déconseillée sur des réseaux ouverts lorsque le service de transport sous-jacent ne peut pas garantir la confidentialité. Les mises en œuvre de LDAP NE DEVRAIENT PAS prendre en charge par défaut les méthodes d'authentification qui utilisent des mots de passe en clair et autres accréditifs d'authentification non protégés sauf si les données sur la session sont protégées en utilisant TLS ou autres protections de la confidentialité et de l'intégrité des données.

La transmission de mots de passe en clair -- normalement pour authentification ou modification – présente un risque significatif pour la sécurité. Ce risque peut être évité en utilisant le mécanisme d'authentification SASL [RFC4422] qui ne transmet pas de mots de passe en clair, ou en négociant des services de confidentialité des données à la couche transport ou session avant de transmettre les valeurs des mots de passe.

Pour atténuer les risques pour la sécurité associés au transfert de mots de passe, une mise en œuvre de serveur qui prend en charge un mécanisme d'authentification quelconque fondé sur le mot de passe qui transmet des mots de passe en clair DOIT prendre en charge un mécanisme de politique qui exige, au moment de l'authentification ou de la modification du mot de passe, que :
une couche TLS ait été installée avec succès,
OU
un autre mécanisme de protection de la confidentialité des données qui protège la valeur du mot de passe contre l'espionnage ait été fourni,
OU
le serveur retourne un code de résultat de confidentialityRequired pour l'opération (c'est-à-dire, nom/mot de passe Bind avec valeur de mot de passe, Bind SASL transmettant une valeur de mot de passe en clair, ajout ou modification incluant une valeur de userPassword, etc.), même si la valeur du mot de passe est correcte.

Les mises en œuvre de serveurs peuvent aussi vouloir fournir des mécanismes de politique pour invalider ou autrement protéger les comptes dans des situations où un serveur détecte qu'un mot de passe pour un compte a été transmis en clair.

6.3.4 Considérations sur la sécurité de hachage de mot de passe

Certains mécanismes d'authentification (par exemple, DIGEST-MD5) transmettent un hachage de la valeur du mot de passe qui peut être vulnérable à des attaques hors ligne par recherche exhaustive. Les développeurs devraient veiller à protéger de telles valeurs hachées de mot de passe durant une transmission en utilisant TLS ou d'autres mécanismes de confidentialité.

6.4 Considérations sur la sécurité de SASL

Tant qu'un service de protection de l'intégrité des données n'est pas installé sur une session LDAP, un attaquant peut modifier les valeurs transmises de la réponse d'attribut 'supportedSASLMechanisms' et donc dégrader la liste des mécanismes SASL disponibles pour n'y inclure que les mécanismes les moins sûrs. Pour détecter ce type d'attaque, le client peut restituer les mécanismes SASL que le serveur rend disponibles à la fois avant et après l'installation d'un service de protection de l'intégrité des données sur une session LDAP. Si le client trouve que la liste de ce qui est protégé en intégrité (la liste obtenue après l'installation du service d'intégrité des données) contient un mécanisme plus

fort que celui de la liste obtenue précédemment, le client devrai supposer que la liste obtenue précédemment a été modifiée par un attaquant. Dans ces circonstances, il est recommandé que le client ferme la connexion de transport sous-jacente et se reconnecte en suite pour rétablir la session.

6.5 Considérations connexes sur la sécurité

On trouvera dans les [RFC4422], [RFC4013], [RFC3454], et [RFC3629] des considérations supplémentaires sur la sécurité qui se rapportent et s'appliquent à diverses méthodes et mécanismes d'authentification exposés dans le présent document.

7 Considérations relatives à l'IANA

L'IANA a mis à jour le registre du mécanisme de protocole LDAP pour indiquer que le présent document et la [RFC4511] donnent la spécification technique définitive pour l'opération étendue StartTLS (1.3.6.1.4.1.1466.20037).

L'IANA a mis à jour le registre des types LDAPMessage LDAP pour indiquer que le présent document et la [RFC4511] donnent la spécification technique définitive pour les types de message bindRequest (0) et bindResponse (1).

L'IANA a mis à jour le registre de méthode d'authentification Bind LDAP pour indiquer que le présent document et la [RFC4511] donnent la spécification technique définitive pour les méthodes d'authentification Bind simple (0) et sasl (3).

L'IANA a mis à jour le registre des préfixes authzid LDAP pour indiquer que le présent document donne la spécification technique définitive pour les préfixes authzid dnAuthzId (dn:) et uAuthzId (u:).

8 Remerciements

Le présent document combine des informations contenues à l'origine dans les RFC 2251, RFC 2829, et RFC 2830. La RFC 2251 était un produit du groupe de travail Accès, Recherche, et Indexage des Répertoires (ASID, *Access, Searchin, Indexing of Directories*). Les RFC 2829 et RFC 2830 ont été produites par le groupe de travail extensions LDAP (LDAPEXT).

Le présent document est un produit du groupe de travail Révision de LDAP (LDAPBIS) de l'IETF.

9 Références normatives

[RFC791] Postel, J., "Internet Protocol", STD 5, RFC 791, septembre 1981.

[RFC2119] Bradner, S., "Mots clé à utiliser dans les RFC pour indiquer les niveaux d'exigence", BCP 14, RFC 2119, mars 1997.

[RFC2460] Deering, S. et R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, décembre 1998.

[RFC3454] Hoffman, P. et M. Blanchet, "Preparation of Internationalized Strings ("stringprep")", RFC 3454, décembre 2002.

[RFC3490] Faltstrom, P., Hoffman, P., et A. Costello, "Internationalizing Domain Names in Applications (IDNA)", RFC 3490, mars 2003.

[RFC3629] Yergeau, F., "UTF-8, a transformation format of ISO 10646", STD 63, RFC 3629, novembre 2003.

[RFC4013] Zeilenga, K., "SASLprep: Stringprep Profile for User Names et Passwords", RFC 4013, février 2005.

[RFC4234] Crocker, D. et P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 4234, octobre 2005.

[RFC4346] Dierks, T. et E. Rescorla, "The TLS Protocol Version 1.1", RFC 4346, mars 2006.

[RFC4422] Melnikov, A., Ed. et K. Zeilenga, Ed., "Simple authentication et Security Layer (SASL)", RFC 4422, juin 2006.

[RFC4510] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map", RFC 4510, juin 2006.

[RFC4511] Sermersheim, J., Ed., "Lightweight Directory Access Protocol (LDAP): The Protocol", RFC 4511, juin 2006.

[RFC4512] Zeilenga, K., "Lightweight Directory Access Protocol (LDAP): Directory Information Models", RFC 4512, juin 2006.

[RFC4514] Zeilenga, K., Ed., "Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names", RFC 4514, juin 2006.

[RFC4517] Legg, S., Ed., "Lightweight Directory Access Protocol (LDAP): Syntaxes et Matching Rules", RFC 4517, juin 2006.

[RFC4519] Sciberras, A., Ed., "Lightweight Directory Access Protocol (LDAP): Schema for User Applications", RFC 4519, juin 2006.

[RFC4520] Zeilenga, K., "Internet Assigned Numbers Authority (IANA) Considerations for the Lightweight Directory Access Protocol (LDAP)", BCP 64, RFC 4520, juin 2006.

[Unicode] The Unicode Consortium, "The Unicode Standard, Version 3.2.0" is defined by "The Unicode Standard, Version 3.0" (Reading, MA, Addison-Wesley, 2000. ISBN 0-201-61633-5), as amended by the "Unicode Standard Annex #27: Unicode 3.1" (http://www.unicode.org/reports/tr27/) et by the "Unicode Standard Annex #28: Unicode 3.2" (http://www.unicode.org/reports/tr28/).

[X.501] ITU-T Rec. X.501, "The Directory: Models", 1993.

10 Références informatives

[DIGEST-MD5] Leach, P., Newman, C., et A. Melnikov, "Using Digest L’authentification as a SASL Mechanism", Work in Progress, March 2006.

[PLAIN] Zeilenga, K., "The Plain SASL Mechanism", Work in Progress, mars 2005.

[RFC2828] Shirey, R., "Internet Security Glossary", FYI 36, RFC 2828, mai 2000.

[RFC4301] Kent, S. et K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, décembre 2005.

[RFC4505] Zeilenga, K., "The Anonymous SASL Mechanism", RFC 4505, juin 2006.

Appendice A
Concepts d’authentification et d’autorisation

Le présent appendice n’est pas normatif.

Le présent appendice définit les termes, concepts, et interrelations de base concernant l’authentification, l’autorisation, les accréditifs, et l’identité. Ces concepts sont utilsés por décrire comment diverses approches de sécurité sont utilisées dans l’authentification et l’autorisation de client.

A.1 Politique de contrôle d'accès

Une politique de contrôle d'accès est une ensemble de règles définissant la protection de ressources, généralement en termes de capacités des personnes ou autres entités qui accèdent à ces ressources. Les objets et mécanismes de sécurité, tels que ceux décrits ici, activent l'expression des politiques de contrôle d'accès et leur mise en œuvre.

A.2 Facteurs de contrôle d'accès

Une demande, lorsqu'elle est traitée par un serveur, peut être associée à une grande variété de facteurs en rapport avec la sécurité. Le serveur utilise ces facteurs pour déterminer s'il convient de traiter la demande et comment le faire. C'est ce qu'on appelle les facteurs de contrôle d'accès (ACF, *access control factor*). Ils peuvent inclure une adresse IP de source, la force du chiffrement, le type d'opération demandée, l'heure, etc.. Certains facteurs peuvent être spécifiques de la demande elle-même ; d'autres peuvent être associés à la connexion transport via laquelle est transmise la demande ; et d'autres (par exemple, l'heure) peuvent être "environnementaux".

Les politiques de contrôle d'accès sont exprimées en termes de facteurs de contrôle d'accès ; par exemple, "une demande ayant les ACF i,j,k peut effectuer l'opération Y sur la ressource Z". L'ensemble des ACFs qu'un serveu rend disponibles pour de telles expressions est spécifique de la mise en œuvre.

A.3 Authentification, accréditifs, identité

Les accréditifs d'authentification sont les preuves fournies par une partie à une autre, qui affirment l'identité de la partie productrice (par exemple, un utilisateur) qui essaye d'établir un nouvel état d'autorisation avec l'autre partie (normalement, un serveur). L'authentification est le processus de générer, transmettre, et vérifier ces accréditifs et donc l'identité qu'ils affirment. Une identité d'authentification est le nom présenté dans un accréditif.

Il y a de nombreuses formes d'accréditifs d'authentification. La forme utilisée dépend du mécanisme d'authentification particulier négocié par les parties. Les certificats X.509, les tickets Kerberos, et de simples paires identité et mot de passe sont tous des exemples de formes d'accréditifs d'authentification. Noter qu'un mécanisme d'authentification peut contraindre la forme des identités d'authentification utilisées avec elles.

A.4 Identité d'autorisation

Une identité d'autorisation est une forme de facteur de contrôle d'accès. Elle est le nom de l'utilisateur ou autre entité qui demande que soit effectuée ces opérations. Les politiques de contrôle d'accès sont souvent exprimées en termes d'identités d'autorisation ; par exemple, "l'entité X peut effectuer l'opération Y sur la ressource Z".

L'identité d'autorisation d'une session LDAP est souvent sémantiquement la même que l'identité d'authentification présentée par le client, mais elle peut être différente. SASL permet aux clients de spécifier une identité d'autorisation distincte de l'identité d'authentification affirmée par les accréditifs du client. Cela permet à des agents tels que des serveurs mandataires de s'authentifier en utilisant leurs propres accréditifs, et par là de demander les privilèges d'accès de l'identité au nom de laquelle ils sont mandatés [RFC4422].

La forme de l'identité d'authentification fournie par un service comme TLS peut aussi ne pas correspondre aux identités d'autorisation utilisées pour exprimer une politique ce contrôle d'accès au serveur, et donc d'effectuer une transposition spécifique du serveur. La méthode par laquelle un serveur compose et valide une identité d'autorisation à partir des accréditifs d'authentification fournis par un client est spécifique de la mise en œuvre.

Appendice B : Résumé des modifications

Le présent appendice n'est pas normatif.

Le présent appendice résume les changements substantiels faits sur les RFC 2251, RFC 2829 et RFC 2830. En plus des shangements spécifiques décrits ci-dessous, le lecteur du présent document devrait être averti que de nombreuses modifications rédactionnelles générales ont été faites sur le contenu d'origine à partir des documents de source. Ces changements incluent ce qui suit :

- Le matériau d'origine des paragraphes 4.2.1 et 4.2.2 de la RFC 2251, la RFC 2829 (tout sauf les Sections 2 et 4), et la RFC 2830 ont été combinées en un seul document.

- Les matériaux combinés ont été substantiellement réorganisés et édités en groupe de sujets, le flux du document a été amélioré et les intentions précisées.
- Des changements ont été faits tout au long du texte pour respecter les définitions des couches de protocole LDAP et la terminologie de sécurité de l'IETF.
- Des mises à jour et ajouts substantiels ont été fait aux considérations de sécurité à partir des deux documents sur la base de l'expérience du fonctionnement courant.

B.1 Changements par rapport à la RFC 2251

Ce paragraphe résume les changements substantiels faits aux paragraphes 4.2.1 et 4.2.2 de la RFC 2251 par le présent document. Des changements substantiels au paragraphe 4.2.1 de la RFC 2251 sont aussi mentionnés en [RFC4511].

B.1.1 Paragraphe 4.2.1 ("Séquençage de la demande Bind")

- Alinéa 1 : Retirer la phrase, "Si à un stade quelconque le client souhaite interrompre le processus de liaison, il PEUT délier et puis abandonner la connexion sous-jacente". L'opération Unbind permet toujours ce comportement, mais elle n'est pas documentée explicitement.

- Précisé que la session est passée à un état anonyme à réception du PDU BindRequest et qu'elle est seulement passée à un état non anonyme si, et lorsque, la demande Bind est réussie.

B.1.2. Paragraphe 4.2.2 ("Authentification et autres services de sécurité")

- La RFC 2251 établit que l'authentification anonyme DOIT être effectuée en utilisant la méthode Bind simple. La présente spécification définit le mécanisme d'authentification anonyme de la méthode Bind simple et exige de toutes les mises en œuvre conformes qu'elles la prennent en charge. D'autres mécanismes d'authentification produisant l'authentification et l'état d'autorisation anonyme peuvent aussi être appliqués et utilisés par les mises en œuvre conformes.

B.2 Changements par rapport à la RFC 2829

Ce paragraphe résume les changements de de substance faits par rapport à la RFC 2829.

B.2.1. Paragraphe 4 ("Mécanismes de sécurité exigés")

- Le mécanisme d'authentification nom/mot de passe (voir le paragraphe B.2.5 ci-dessous) protégé par TLS remplace le mécanisme DIGEST-MD5 de SASL comme mécanisme d'authentification fondé sur le mot de passe d'application obligatoire pour LDAP. Les mises en œuvre sont encouragées à continuer de prendre en charge DIGEST-MD5 [DIGEST-MD5] pour SASL.

B.2.2. Paragraphe 5.1 ("Procédure d'authentification anonyme")

- Il est précisé que l'authentification anonyme implique une valeur de nom de longueur zéro et une valeur de mot de passe de longueur zéro. Le mécanisme d'authentification non authentifié a été ajouté pour traiter la valeur de mot de passe simple de longueur zéro.

B.2.3. Paragraphe 6 ("Authentification fondée sur le mot de passe")

- Voir au paragraphe B.2.1.

B.2.4. Paragraphe 6.1 ("Authentification par résumé")

- Comme le mécanisme SASL-DIGEST-MD5 n'est plus de mise en œuvre obligatoire, ce paragraphe n'a plus qu'un intérêt historique et n'a pas été inclus dans le présent document. Le paragraphe 6.1 de la RFC 2829, continue de documenter le mécanisme d'authentification SASL DIGEST-MD5.

B.2.5. Paragraphe 6.2 ("Choix d'authentification 'simple' sous chiffrement TLS")

- Renommé le mécanisme d'authentification "simple" en mécanisme d'authentification par nom/mot de passe pour mieux le décrire.

- L'utilisation de TLS a été généralisée pour l'aligner avec les définitions des couches de protocole LDAP. L'établissement de TLS est maintenant exposé comme un sujet indépendant et est généralisé pour être utilisé avec tous les mécanismes d'authentification et autres couches de sécurité.

- Retirée l'implication que l'attribut userPassword serait la seule localisation pour la mémorisation des valeurs de mot de passe à utiliser dans l'authentification. Il n'y a plus aucune exigence impliquée dans la façon ou le lieu où les mots de passe sont mémorisés au serveur pour les utilisations d'authentification.

B.2.6. Paragraphe 6.3 ("Autres choix d'authentification avec TLS")

- Voir au paragraphe B.2.5.

B.2.7. Section 7.1 ("Authentification fondée sur le certificat avec TLS")

- Voir au paragraphe B.2.5.

B.2.8. Paragraphe 8 ("Autres mécanismes")

- Tous les mécanismes d'authentification SASL sont explicitement permis au sein de LDAP. Précisément, cela signifie que les mécanismes SASL ANONYMOUS et SASL PLAIN ne sont plus interdits d'utilisation au sein de LDAP.

B.2.9. Paragraphe 9 ("Identité d'autorisation")

- Les règles de correspondance spécifiées pour les valeurs dnAuthzId et uAuthzId. En particulier, la valeur du nom distinctif dans la forme dnAuthzId doit être satisfaite en utilisant les règles de correspondance de nom distinctif, et la valeur uAuthzId DOIT être préparée en utilisant les règles SASLprep avant d'être comparées octet par octet.

- Précision que les valeurs uAuthzId ne devraient pas être supposées être uniques au monde.

B.2.10. Paragraphe 10 ("Suites de chiffrement TLS")

- Les recommandations sur les suites de chiffrement TLS ne sont plus incluses dans la présente spécification. Les mises en œuvre doivent maintenant prendre en charge la suite de chiffrement TLS_RSA_WITH_3DES_EDE_CBC_SHA et devraient continuer à prendre en charge la suite de chiffrement TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA.

- Il est précisé que l'authentification anonyme implique une valeur de nom de longueur zéro et une valeur de mot de passe de longueur zéro. Le mécanisme d'authentification non authentifié a été ajouté pour traiter les demandes Bind simples impliquant une valeur de nom avec une longueur différente de zéro et une valeur de mot de passe de longueur zéro.

B.3 Changements par rapport à la RFC 2830

Ce paragraphe résume les changements de substance faits aux Sections 3 et 5 de la RFC 2830. Les lecteurs devraient consulter la [RFC4511] pour un résumé des changements aux autres sections.

B.3.1. Paragraphe 3.6 ("Vérification d'identité du serveur")

- Mise à jour substantielle de l'algorithme de vérification de l'identité du serveur pour s'assurer qu'elle est complète et robuste. En particulier, l'utilisation de toutes les valeurs pertinentes dans les champs subjectAltName et subjectName est couverte par l'algorithme et les règles de correspondance sont spécifiées pour chaque type de valeur. Les formes transposées (déduites) de l'identité du serveur peuvent maintenant être utilisées lorsque la transposition est effectuée de façon sécurisée.

B.3.2. Paragraphe 3.7 ("Rafraîchissement des informations de capacités du serveur")

- Les clients ne sont plus obligés de toujours rafraîchir les informations sur les capacités du serveur à la suite de l'établissement de TLS. Ceci est permis pour les situations où ces informations étaient obtenus par un mécanisme sécurisé.

B.3.3. Paragraphe 5 ("Effets de TLS sur l'identité d'autorisation d'un client")

- Etablir une couche TLS sur une session LDAP peut maintenant causer le changement de l'état d'autorisation de la session LDAP.

B.3.4. Paragraphe 5.2 ("Effets de la clôture de la connexion TLS")

- La clôture d'une couche TLS sur une session LDAP change l'état d'authentification et d'autorisation de la session LDAP sur la base de la politique locale. Précisément, cela signifie que les mises en œuvre ne sont pas obligées de changer les états d'authentification et d'autorisation en anonyme à la clôture de TLS.

- Les références à la RFC 2401 sont remplacées par la RFC 4301.

Adresse de l'auteur

Roger Harrison
Novell, Inc.
1800 S. Novell Place
Provo, UT 84606
USA
téléphone : +1 801 861 2642
mél : roger_harrison@novell.com

Déclaration de copyright

Propriété intellectuelle

Remerciement

Le financement de la fonction d'édition des RFC est actuellement fourni par l'activité de soutien administratif de l'IETF (IASA, *Administrative Support Activity*).